

УДК 519.714.1

УТОЧНЕНИЕ НИЖНЕЙ ОЦЕНКИ СЛОЖНОСТИ ВОЗВЕДЕНИЯ В СТЕПЕНЬ

В. В. Кочергин, Д. В. Кочергин

Московский государственный университет имени М. В. Ломоносова, г. Москва, Россия

Для величины $l(x^n)$ — минимального числа операций умножения, достаточного для вычисления по переменной x степени x^n — уточнена нижняя оценка. Установлено, что для любого $\varepsilon > 0$ доля чисел k , не превосходящих n и удовлетворяющих условию

$$l(x^k) > \log_2 n + \frac{\log_2 n}{\log_2 \log_2 n} \left(1 - (2 + \varepsilon) \frac{\log_2 \log_2 \log_2 n}{\log_2 \log_2 n} \right),$$

стремится к 1 при $n \rightarrow \infty$.

Ключевые слова: аддитивные цепочки, возведение в степень, нижние оценки сложности.

DOI 10.17223/20710410/38/10

IMPROVEMENT OF THE LOWER BOUND FOR THE COMPLEXITY OF EXPONENTIATION

V. V. Kochergin, D. V. Kochergin

*Lomonosov Moscow State University, Moscow, Russia***E-mail:** vvkoch@yandex.ru, dk@kocherg.in

Let $l(x^n)$ be the minimal number of multiplications sufficient for computing x^n . In the paper, we improve the lower bound of $l(x^n)$. We establish that for all $\varepsilon > 0$ the fraction of the numbers k , $k \leq n$, satisfying the relation

$$l(x^k) > \log_2 n + \frac{\log_2 n}{\log_2 \log_2 n} \left(1 - (2 + \varepsilon) \frac{\log_2 \log_2 \log_2 n}{\log_2 \log_2 n} \right),$$

tends to 1 as $n \rightarrow \infty$.

Keywords: addition chains, exponentiation, lower bounds of complexity.

1. Определения, обсуждения, формулировка основного результата

В работе исследуется возможность уточнения нижней оценки для известной (см., например, [1, разд. 4.6.3]) задачи о сложности возведения в степень, т. е. задачи о нахождении величины $l(x^n)$ — минимального числа операций умножения, достаточного для вычисления по переменной x степени x^n .

Эту задачу (а также её обобщения) обычно рассматривают в аддитивной постановке — это так называемая задача об аддитивных цепочках [2], которая формулируется следующим образом. *Аддитивной цепочкой* для натурального числа n называется всякая последовательность целых чисел

$$a_0 = 1, a_1, \dots, a_m = n,$$

удовлетворяющая следующему свойству: для каждого k , $1 \leq k \leq m$, найдутся два целых числа (не обязательно различных) i и j , $0 \leq i \leq k-1$, $0 \leq j \leq k-1$, таких, что $a_k = a_i + a_j$. Минимальная длина m аддитивной цепочки для n называется *аддитивной сложностью* числа n и обозначается $l(n)$. Очевидно, что величины $l(n)$ и $l(x^n)$ равны.

Различным аспектам классической задачи об эффективном вычислении степеней (задачи о длине аддитивных цепочек) посвящено большое число публикаций (см., например, работы [1, 3–11], являющиеся обзорами или содержащие обзорную часть). Кроме того, в связи с активным применением аппарата аддитивных цепочек в криптографических алгоритмах и других приложениях [12–14] в последнее время объём литературы по этой тематике серьёзно увеличился. В значительной части публикаций приводятся разные эвристические алгоритмы возведения в степень (построения аддитивных цепочек), но принципиальных улучшений оценок величины $l(x^n)$, доказанных в середине прошлого века, практически не получено.

В 1939 г. А. Брауэром [15] для величины $l(n)$ при $n \rightarrow \infty$ установлена асимптотическая формула

$$l(n) \sim \log n$$

и получена верхняя оценка

$$l(n) \leq \log n + \frac{\log n}{\log \log n} \left(1 + \frac{2 \log \log \log n}{\log \log n} + \frac{1 + o(1)}{\log \log n} \right). \quad (1)$$

Здесь и далее $\log x$ — это $\log_2 x$, а запись $f(n) \sim g(n)$ означает, что при $n \rightarrow \infty$ отношение $f(n)/g(n)$ стремится к 1.

В 1960 г. П. Эрдёш [16] показал, что для любого $\varepsilon > 0$ найдётся такая константа c , $1 < c < 2$, что доля чисел n , не превосходящих N и удовлетворяющих условию

$$l(n) > \log N + (1 - \varepsilon) \frac{\log N}{\log \log N},$$

а, следовательно, и условию

$$l(n) > \log n + (1 - \varepsilon) \frac{\log n}{\log \log n}, \quad (2)$$

при всех достаточно больших значениях n не меньше величины $1 - (c/2)^{\log n}$ и, как следствие, стремится к 1 при $n \rightarrow \infty$ (похожий, но более слабый результат установлен в [17]).

Стоит отметить разную природу слагаемых в правой части неравенства (2) — слагаемое $\log n$ связано с величиной числа n и должно присутствовать для любого значения n , а «мощностное» (отношение логарифма количества чисел, не превосходящих n , к повторному логарифму) слагаемое зависит от «строения» числа n и присутствует для «почти всех» n . Однако несмотря на то, что для почти всех значений n величина $l(n) - \log n$ достаточно велика, предъявить явным образом бесконечную последовательность таких значений не удаётся. Конструктивных нижних оценок, качественно сильнее неравенства

$$l(n) \geq \log n + \log s(n) - 2,13$$

(здесь $s(n)$ — число единиц в двоичной записи числа n), установленного в 1975 г. А. Шенхаге [18], до сих пор, по-видимому, не получено.

Такая ситуация (принципиальная разница между типичным значением сложности и известными нижними оценками сложности для конкретных представителей) характерна для схемных вычислений [19, 20].

Сравним результаты о типичных значениях сложности вычисления степеней с аналогичными результатами в хорошо изученной задаче о сложности реализации булевых функций схемами из функциональных элементов (логическими схемами, булевыми схемами).

О. Б. Лупановым найдена (см., например, [21], где можно найти все необходимые определения) асимптотика роста функции Шеннона $L_B(n)$, характеризующей сложность (минимальное число элементов) реализации схемами в произвольном полном конечном базисе B самой сложнореализуемой функции от n переменных. Из этого результата для произвольного полного базиса B_1 , состоящего из функций, зависящих не более чем от двух переменных, можно извлечь следующие оценки:

$$\begin{aligned} L_{B_1}(n) &\leq \frac{H_1(n)}{\log H_1(n)} \left(1 + (3 + o(1)) \frac{\log \log H_1(n)}{\log H_1(n)} \right), \\ L_{B_1}(n) &\geq \frac{H_1(n)}{\log H_1(n)} \left(1 + (1 + o(1)) \frac{\log \log H_1(n)}{\log H_1(n)} \right), \end{aligned} \quad (3)$$

где $H_1(n)$ — двоичный логарифм числа объектов из реализуемого класса (множества булевых функций от n переменных), т. е. $H_1(n) = 2^n$. Отметим, что нижняя оценка величины $L_B(n)$ выводится стандартным мощностным методом, восходящим применительно к рассматриваемой тематике, по-видимому, к работе [22], и справедлива для «почти всех» функций от n переменных, в то время как все известные нижние оценки для эффективно задаваемых функций не более чем линейны.

С. А. Ложкиным в работе [23] дано краткое схематичное описание метода, позволяющего следующим образом усилить верхнюю оценку:

$$L_{B_1}(n) \leq \frac{H_1(n)}{\log H_1(n)} \left(1 + (1 + \kappa_{B_1} + o(1)) \frac{\log \log H_1(n)}{\log H_1(n)} \right),$$

где $\kappa_B = 1$ в случае, когда базис B симметричный [3], и $\kappa_B = 0$ в остальных случаях.

В [24] анонсировано получение такой верхней оценки, которая вместе с мощностной нижней оценкой (1) даёт равенство

$$L_{B_1}(n) = \frac{H_1(n)}{\log H_1(n)} \left(1 + (1 + o(1)) \frac{\log \log H_1(n)}{\log H_1(n)} \right). \quad (4)$$

Таким образом, если следовать [24], то для функции Шеннона сложности реализации функций алгебры логики схемами над произвольным полным конечным базисом мощностная нижняя оценка, записанная в виде (3), принципиально неулучшаема.

Однако для ещё одной модели схемных вычислений — сборки слов схемами конкатенации [25] — выявлена возможность усиления аналога мощностной нижней оценки из соотношения (4).

Схемы конкатенации можно рассматривать как схемы, имеющие два входа, на которые подаются символы 0 и 1, а каждому элементу схемы соответствует операция конкатенации. Под величиной $L^c(S)$ понимается общее число элементов схемы S , сложность двоичного слова $\tilde{\alpha}$ определяется равенством $L^c(\tilde{\alpha}) = \min L^c(S)$, где минимум берётся по всем схемам конкатенации, реализующим слово $\tilde{\alpha}$, а соответствующая функция

Шеннона — равенством $L^c(n) = \max L^c(\tilde{\alpha})$, где максимум берётся по всем двоичным словам $\tilde{\alpha}$ длины n .

При аккуратном применении известных методов можно получить следующие верхнюю и нижнюю оценки:

$$\begin{aligned} L^c(n) &\leq \frac{H_2(n)}{\log H_2(n)} \left(1 + (2 + o(1)) \frac{\log \log H_2(n)}{\log H_2(n)} \right), \\ L^c(n) &\geq \frac{H_2(n)}{\log H_2(n)} \left(1 + (1 + o(1)) \frac{\log \log H_2(n)}{\log H_2(n)} \right), \end{aligned} \quad (5)$$

где $H_2(n)$ — двоичный логарифм числа объектов из реализуемого класса (слов длины n), т. е. $H_2(n) = n$.

Мощностная нижняя оценка (5) имеет такой же вид, что и нижняя оценка (3). Однако в отличие от случая реализации булевых функций, для задачи о сложности сборки слов схемами конкатенации нижняя оценка может быть усилена [25]: при $n \rightarrow \infty$ справедливо равенство

$$L^c(n) = \frac{H_2(n)}{\log H_2(n)} \left(1 + (2 + o(1)) \frac{\log \log H_2(n)}{\log H_2(n)} \right). \quad (6)$$

Возвращаясь к исходной задаче об аддитивных цепочках, заметим, что из результатов Брауэра (неравенство (1)) и Эрдёша для соответствующей функции Шеннона $L^a(n)$ аддитивной сложности множества натуральных чисел, не превосходящих n , определяемой равенством

$$L^a(n) = \max_{k:k \leq n} l(k),$$

непосредственно следуют оценки

$$\begin{aligned} L^a(n) &\leq H_3(n) + \frac{H_3(n)}{\log H_3(n)} \left(1 + (2 + o(1)) \frac{\log \log H_3(n)}{\log H_3(n)} \right), \\ L^a(n) &\geq H_3(n) + (1 - o(1)) \frac{H_3(n)}{\log H_3(n)}, \end{aligned} \quad (7)$$

где $H_3(n)$ — двоичный логарифм числа натуральных чисел, не превосходящих n , т. е. $H_3(n) = \log n$.

Возникает вопрос: можно ли в нижней оценке (7) величины $L^a(n)$ мощностную составляющую усилить подобно нижней оценке (6) или хотя бы подобно нижним оценкам (3) и (5)? Этот вопрос оказался весьма трудным. Трудности связаны с наличием в оценке (7) слагаемых двух типов, которое приводит к большому разнообразию схем с заданной «мощностной» составляющей сложности. В этом направлении удалось получить следующее продвижение.

Обозначим через $R(m, \varepsilon)$ число возрастающих аддитивных цепочек

$$1 = a_0, a_1, a_2, \dots, a_r, \quad (8)$$

удовлетворяющих условиям

$$\lfloor \log a_r \rfloor = m; \quad (9)$$

$$r \leq m + \frac{m}{\log m} - (2 + \varepsilon) \frac{m \log \log m}{(\log m)^2}. \quad (10)$$

Лемма 1. Для любого положительного значения ε при $m \rightarrow \infty$ выполняется соотношение

$$\frac{R(m, \varepsilon)}{2^m} \rightarrow 0.$$

Эта лемма является основным содержательным утверждением работы, её доказательство приводится в п. 2. Непосредственно из леммы 1 следует

Теорема 1. Пусть $n \rightarrow \infty$. Тогда

$$L^a(n) \geq \log n + \frac{\log n}{\log \log n} \left(1 - (2 + o(1)) \frac{\log \log \log n}{\log \log n} \right).$$

Следствие 1. При $n \rightarrow \infty$ выполняется соотношение

$$\left| L^a(n) - \left(\log n + \frac{\log n}{\log \log n} \right) \right| \leq (2 + o(1)) \frac{\log n \log \log \log n}{(\log \log n)^2}.$$

Последнее неравенство, непосредственно вытекающее из теоремы 1 и верхней оценки Брауэра, может быть переписано в удобном для сравнения с оценками функций Шеннона сложности реализации булевых функций и двоичных наборов виде таким образом:

$$\left| L^a(n) - \left(H_3(n) + \frac{H_3(n)}{\log H_3(n)} \right) \right| \leq (2 + o(1)) \frac{H_3(n) \log \log H_3(n)}{(\log H_3(n))^2}. \quad (11)$$

Итак, установлена нижняя оценка, имеющая для почти всех значений n точно такое же по абсолютной величине отклонение от $\log n + (\log n)/(\log \log n)$, как и отклонение в верхней оценке Брауэра из (1).

2. Доказательство основной леммы

В основе доказательства леммы 1 лежат рассуждения из [16] (см. также [1, разд. 4.6.3]).

Положим

$$\delta = \delta(m) = 2^{\frac{\varepsilon \log \log m}{4 \log m}} - 1. \quad (12)$$

Поскольку $\delta \rightarrow 0$ при $m \rightarrow \infty$, будем считать, что

$$\delta < \sqrt{2} - 1. \quad (13)$$

Разобьём r шагов произвольной возрастающей цепочки (8), удовлетворяющей условиям (9) и (10), на три класса.

Шаг i отнесём к *первому классу*, если этот шаг является удвоением, т. е. $a_i = 2a_{i-1}$.

Шаг i отнесём ко *второму классу*, если

$$\begin{aligned} a_i &< 2a_{i-1}, \\ a_i &\geq (1 + \delta)^{i-j} a_j \text{ для всех } j \text{ } (0 \leq j < i). \end{aligned}$$

Шаг i отнесём к *третьему классу*, если

$$\begin{aligned} a_i &< 2a_{i-1}, \\ a_i &< (1 + \delta)^{i-j} a_j \text{ для некоторого } j \text{ } (0 \leq j < i). \end{aligned} \quad (14)$$

Шаги, отнесённые к первому классу, будем называть удвоениями, а к третьему — мини-шагами. Количество шагов в классах обозначим соответственно через u_1 , u_2 и u_3 . Очевидно, что $u_1 + u_2 + u_3 = r$.

Оценим сверху величину $u_2 + u_3$. Если шаг i отнесён ко второму или третьему классу, то $a_i \neq 2a_{i-1}$, т. е. $a_i \leq a_{i-1} + a_{i-2} \leq 3a_{i-2}$. Используя (9) и (13), получаем

$$2^m \leq a_r < 3^{(u_2+u_3)/2} 2^{u_1} = \frac{2^{u_1+u_2+u_3}}{(4/3)^{(u_2+u_3)/2}} = \frac{2^r}{2^{(u_2+u_3+u_4) \log(2/\sqrt{3})}}.$$

Поэтому в силу (10)

$$u_2 + u_3 < \frac{1}{\log(2/\sqrt{3})} (r - m) \leq \frac{1}{\log(2/\sqrt{3})} \frac{2m}{\log m} < 10 \frac{m}{\log m}.$$

Теперь оценим сверху величину u_3 . Для каждого мини-шага i_s ($s = 1, \dots, u_3$) при соответствующем j_s ($0 \leq j_s \leq i_s$) в силу (14) выполняется неравенство $a_{i_s} < a_{j_s} (1 + \delta)^{i_s - j_s}$. Пусть $I_1, \dots, I_{u_3}$ — полуинтервалы $(j_1, i_1], \dots, (j_{u_3}, i_{u_3}]$, где $(j, i]$ — множество целых чисел ρ , таких, что $j < \rho \leq i$. Построим систему неперекрывающихся полуинтервалов $J_1 = (j'_1, i'_1], \dots, J_h = (j'_h, i'_h]$, такую, что

$$I_1 \cup \dots \cup I_{u_2} = J_1 \cup \dots \cup J_h, \\ a_{i'_s} < a_{j'_s} (1 + \delta)^{2(i'_s - j'_s)} \text{ для } 1 \leq s \leq h.$$

Пусть $i_1 < i_2 < \dots < i_{u_2}$. Удалим все полуинтервалы I_t , которые можно удалить, не сужая множество $I_1 \cup \dots \cup I_{u_2}$. Каждую систему перекрывающихся полуинтервалов $(j_c, i_c], \dots, (j_d, i_d]$ объединим в один полуинтервал $(j', i'] = (j_c, i_d]$. Заметим, что

$$a_{i'} < a_{j'} (1 + \delta)^{i_c - j_c + \dots + i_d - j_d} \leq a_{j'} (1 + \delta)^{2(i' - j')},$$

так как каждая точка полуинтервала $(j', i']$ покрыта полуинтервалами $(j_c, i_c], \dots, (j_d, i_d]$ не более чем дважды.

Положим $q = (i'_1 - j'_1) + \dots + (i'_h - j'_h)$. Обозначим через u'_1 и u'_2 число шагов, относящихся соответственно к первому и второму классам и имеющих номера, принадлежащие множеству $J_1 \cup \dots \cup J_h$. Отметим, что $u'_1 + u'_2 + u_3 = q$. Тогда справедливы соотношения

$$2^m \leq a_r \leq 2^{u_1 - u'_1} 3^{(u_2 - u'_2)/2} (1 + \delta)^{2q} = \\ = 2^{u_1 - u'_1} \left(\frac{\sqrt{3}}{2} \right)^{u_2 - u'_2} 2^{u_2 - u'_2} \left(\frac{(1 + \delta)^2}{2} \right)^{u'_1 + u'_2 + u_3} 2^{u'_1 + u'_2 + u_3} = 2^r \left(\frac{\sqrt{3}}{2} \right)^{u_2 - u'_2} \left(\frac{(1 + \delta)^2}{2} \right)^{u'_1 + u'_2 + u_3}.$$

Отсюда и из (9) и (12) при всех достаточно больших значениях m получаем

$$u_3 \leq \frac{r - m}{1 - 2 \log(1 + \delta)} - \frac{1 - (\log 3)/2}{1 - 2 \log(1 + \delta)} (u_2 - u'_2) - u'_1 - u'_2 \leq \\ \leq \frac{m / \log m - (2 + \varepsilon) m \log \log m / (\log m)^2}{1 - \varepsilon \log \log m / (4 \log m)} - \left(1 - \frac{1}{2} \log 3 \right) (u_2 - u'_2) - u'_1 - u'_2 < \\ < \left(1 + \frac{\varepsilon \log \log m}{3 \log m} \right) \left(\frac{m}{\log m} - (2 + \varepsilon) \frac{m \log \log m}{(\log m)^2} \right) - \left(1 - \frac{1}{2} \log 3 \right) u_2 - u'_1 \leq \\ \leq \frac{m}{\log m} - (2 + \varepsilon/2) \frac{m \log \log m}{(\log m)^2} - \left(1 - \frac{1}{2} \log 3 \right) u_2 - u'_1.$$

Таким образом, если для произвольной возрастающей цепочки (8) выполняются неравенства (9) и (10), то эта цепочка удовлетворяет следующей системе условий:

$$\begin{aligned} u_3 &\leq \frac{m}{\log m} - (2 + \varepsilon/2) \frac{m \log \log m}{(\log m)^2} - \left(1 - \frac{1}{2} \log 3\right) u_2, \\ u_2 + u_3 &\leq 10 \frac{m}{\log m}, \\ u_1 + u_2 + u_3 &\leq m + \frac{m}{\log m} - (2 + \varepsilon) \frac{m \log \log m}{(\log m)^2}. \end{aligned} \quad (15)$$

Отметим, что везде, за исключением выкладок в (36), вместо первого неравенства из совокупности (15) достаточно использовать следующую более грубую оценку величины u_3 :

$$u_3 \leq \frac{m}{\log m} - (2 + \varepsilon/2) \frac{m \log \log m}{(\log m)^2}.$$

Пусть теперь заданы значения u_1, u_2, u_3 , удовлетворяющие условиям (15). Тогда существует не более

$$\binom{u_1 + u_2 + u_3}{u_2 + u_3} \binom{u_2 + u_3}{u_2} \quad (16)$$

способов отнести каждый шаг к тому или иному классу шагов. После того как распределение шагов задано, оценим число возможностей выбора самих шагов. Отметим, что шаги, отнесённые к первому классу, полностью определяются своими номерами.

Сначала оценим сверху число способов выбора шагов, отнесённых ко второму классу. Если i -й шаг отнесён ко второму классу, то в силу (13) выполняется неравенство $a_i \geq (1 + \delta)a_{i-1}$. Пусть $a_i = a_j + a_k$, где $a_j \geq a_k$. Тогда

$$\delta a_{i-1} \leq a_k \leq a_j \leq a_{i-1}. \quad (17)$$

Кроме того, в силу (13)

$$a_j \leq \frac{a_i}{(1 + \delta)^{i-j}} \leq \frac{2a_{i-1}}{(1 + \delta)^{i-j}}, \quad a_k \leq \frac{a_i}{(1 + \delta)^{i-k}} \leq \frac{2a_{i-1}}{(1 + \delta)^{i-k}}. \quad (18)$$

Из (17) и (18) получаем $\delta \leq \frac{2}{(1 + \delta)^{i-j}}$, $\delta \leq \frac{2}{(1 + \delta)^{i-k}}$.

Пусть для некоторого натурального β выполняется неравенство $\delta \leq 2/(1 + \delta)^\beta$. Тогда $\delta(1 + \beta\delta) \leq 2$. Отсюда в силу (12) получаем

$$\beta \leq \frac{2 - \delta}{\delta^2} \leq \frac{2}{\delta^2} = \frac{2}{\left(2^{\frac{\varepsilon \log \log m}{4 \log m}} - 1\right)^2} \leq \frac{32(\log m)^2}{\varepsilon^2 (\ln 2)^2 (\log \log m)^2}.$$

Таким образом, имеется не более

$$(\beta^2)^{u_2} \leq \left(\frac{8 \log m}{\varepsilon \ln 2 \log \log m} \right)^{4u_2} \quad (19)$$

возможностей для выбора шагов из второго класса.

Оценим сверху число способов выбора шагов, отнесённых к третьему классу. После того как определены все шаги из второго класса, имеется не более

$$\binom{r^2}{u_3} \quad (20)$$

возможностей выбора u_3 пар индексов $(j_1, k_1), \dots, (j_{u_3}, k_{u_3})$ для шагов третьего класса. В порядке возрастания номера i для каждого шага из третьего класса используем такую пару (j_h, k_h) из множества $\{(j_1, k_1), \dots, (j_{u_3}, k_{u_3})\}$, для которой выполнены условия $j_h < i$, $k_h < i$ и величина $\max(j_h, k_h)$ принимает наименьшее значение. Если такой пары не существует, или после её использования цепочка перестанет быть возрастающей, или получившийся шаг не является мини-шагом, то аддитивная цепочка не будет получена. При этом любая возрастающая аддитивная цепочка с шагами из третьего класса на назначенных местах будет получена одним из указанных способов.

Учитывая это, получаем, что величина (20) даёт верхнюю оценку для числа вариантов выбора шагов, отнесённых к третьему классу. Таким образом, число возрастающих аддитивных цепочек с заданным количеством u_1 , u_2 и u_3 шагов, отнесённых к первому, второму и третьему классам соответственно, не больше произведения величин (16), (19) и (20), т. е. не превосходит величины

$$\binom{u_1 + u_2 + u_3}{u_2 + u_3} \binom{u_2 + u_3}{u_2} \left(\frac{8 \log m}{\varepsilon \ln 2 \log \log m} \right)^{4u_2} \binom{(u_1 + u_2 + u_3)^2}{u_3}.$$

Поэтому

$$R(m, \varepsilon) \leq \sum \binom{u_1 + u_2 + u_3}{u_2 + u_3} \binom{u_2 + u_3}{u_2} \left(\frac{8 \log m}{\varepsilon \ln 2 \log \log m} \right)^{4u_2} \binom{(u_1 + u_2 + u_3)^2}{u_3}, \quad (21)$$

где сумма берется по всем u_1 , u_2 и u_3 , удовлетворяющим условиям (15).

Для завершения доказательства леммы 1 достаточно установить, что

$$\log R(m, \varepsilon) - m \rightarrow -\infty$$

при $m \rightarrow \infty$. Отдельно оценим сверху каждый множитель (точнее, его логарифм) в слагаемых из правой части неравенства (21).

Оценивая первый множитель, получаем

$$\binom{u_1 + u_2 + u_3}{u_2 + u_3} \leq \frac{(u_1 + u_2 + u_3)^{u_2 + u_3}}{(u_2 + u_3)!} \leq 3^{u_2 + u_3} \left(\frac{u_1 + u_2 + u_3}{u_2 + u_3} \right)^{u_2 + u_3}. \quad (22)$$

Далее рассмотрим два случая. Если выполняется неравенство

$$u_2 + u_3 \leq \frac{m}{\log m \log \log m}, \quad (23)$$

то в силу (15), (22) и (23) справедливы соотношения

$$\begin{aligned} \log \binom{u_1 + u_2 + u_3}{u_2 + u_3} &\leq (u_2 + u_3) \log 3 + (u_2 + u_3) \log(2m) \leq \\ &\leq \frac{m}{\log \log m} + o\left(\frac{m \log \log m}{\log m}\right). \end{aligned} \quad (24)$$

Если же выполняется неравенство

$$u_2 + u_3 > \frac{m}{\log m \log \log m}, \quad (25)$$

то, используя (15), (22) и (25), получаем

$$\begin{aligned} \log \binom{u_1 + u_2 + u_3}{u_2 + u_3} &\leq (u_2 + u_3) \log 3 + (u_2 + u_3) \log(2 \log m \log \log m) \leq \\ &\leq (u_2 + u_3) \log \log m + o\left(\frac{m \log \log m}{\log m}\right). \end{aligned} \quad (26)$$

Логарифм второго множителя произвольного слагаемого из правой части неравенства (21) оценить, учитывая (15), совсем просто:

$$\log \binom{u_2 + u_3}{u_2} \leq u_2 + u_3 = O\left(\frac{m}{\log m}\right) = o\left(\frac{m \log \log m}{\log m}\right). \quad (27)$$

Теперь для всех достаточно больших значений m оценим сверху логарифм третьего множителя:

$$\log \left(\left(\frac{8 \log m}{\varepsilon \ln 2 \log \log m} \right)^{4u_2} \right) \leq 4u_2 \log \log m. \quad (28)$$

И наконец, оценим логарифм четвертого множителя произвольного слагаемого из правой части неравенства (21):

$$\binom{(u_1 + u_2 + u_3)^2}{u_3} \leq \frac{(u_1 + u_2 + u_3)^{2u_3}}{u_3!} \leq 3^{u_3} \left(\frac{(u_1 + u_2 + u_3)^2}{u_3} \right)^{u_3}. \quad (29)$$

Далее рассмотрим два случая. Если выполняется неравенство

$$u_3 \leq \frac{m}{\log m \log \log m}, \quad (30)$$

то в силу (15), (29) и (30) справедливы соотношения

$$\log \binom{(u_1 + u_2 + u_3)^2}{u_3} \leq u_3 \log 3 + u_3 \log(4m^2) \leq \frac{2m}{\log \log m} + o\left(\frac{m \log \log m}{\log m}\right). \quad (31)$$

Если же выполняется неравенство

$$u_3 > \frac{m}{\log m \log \log m}, \quad (32)$$

то, используя (15) и (32), получаем

$$\begin{aligned} \log \binom{(u_1 + u_2 + u_3)^2}{u_3} &\leq u_3 \log 3 + u_3 \log(4m \log m \log \log m) = \\ &= u_3 \log m + u_3 \log \log m + o\left(\frac{m \log \log m}{\log m}\right). \end{aligned} \quad (33)$$

Для оценки величины $R(m, \varepsilon)$ разобьём все слагаемые суммы из (21) на три группы в зависимости от того, каким условиям, помимо (15), удовлетворяют значения u_1 , u_2 и u_3 . Условием вхождения в первую группу является выполнение неравенства

$$u_3 \leq \frac{m}{2 \log m};$$

во вторую группу — неравенств

$$u_3 > \frac{m}{2 \log m}, \quad u_2 \leq \frac{m}{\log m \log \log \log m};$$

в третью группу — выполнение неравенств

$$u_3 > \frac{m}{2 \log m}, \quad u_2 > \frac{m}{\log m \log \log \log m}.$$

Оценим сверху величины слагаемых в каждой группе.

Если слагаемое из правой части неравенства (21) отнесено к первой группе, то, применяя максимальную из оценок (24) и (26), оценки (27) и (28), а также максимальную из оценок (31) и (33), с использованием (15) и (2) имеем

$$\begin{aligned} & \log \left(\binom{u_1 + u_2 + u_3}{u_2 + u_3} \binom{u_2 + u_3}{u_2} \left(\frac{8 \log m}{\varepsilon \ln 2 \log \log m} \right)^{4u_2} \binom{(u_1 + u_2 + u_3)^2}{u_3} \right) \leq \\ & \leq \max \left(\frac{m}{\log \log m}, (u_2 + u_3) \log \log m \right) + 4u_2 \log \log m + \\ & + \max \left(\frac{2m}{\log \log m}, u_3 \log m + u_3 \log \log m \right) + o \left(\frac{m \log \log m}{\log m} \right) \leq \\ & \leq u_3 \log m + 5u_2 \log \log m + 2u_3 \log \log m + O \left(\frac{m}{\log \log m} \right) \leq \frac{m}{2} + O \left(\frac{m}{\log \log m} \right). \end{aligned} \quad (34)$$

Если слагаемое из правой части неравенства (21) отнесено ко второй группе, то выполняются неравенства (25) и (32). Применяя оценки (26), (27), (28) и (33), с использованием (15) и (2) имеем

$$\begin{aligned} & \log \left(\binom{u_1 + u_2 + u_3}{u_2 + u_3} \binom{u_2 + u_3}{u_2} \left(\frac{8 \log m}{\varepsilon \ln 2 \log \log m} \right)^{4u_2} \binom{(u_1 + u_2 + u_3)^2}{u_3} \right) \leq \\ & \leq (u_2 + u_3) \log \log m + 4u_2 \log \log m + u_3 \log m + u_3 \log \log m + o \left(\frac{m \log \log m}{\log m} \right) \leq \\ & \leq u_3 \log m + 5u_2 \log \log m + 2u_3 \log \log m + o \left(\frac{m \log \log m}{\log m} \right) \leq \\ & \leq \left(\frac{m}{\log m} - (2 + \varepsilon/2) \frac{m \log \log m}{(\log m)^2} \right) \log m + \\ & + 2 \left(\frac{m}{\log m} - (2 + \varepsilon/2) \frac{m \log \log m}{(\log m)^2} \right) \log \log m + o \left(\frac{m \log \log m}{\log m} \right) \leq \\ & \leq m - \frac{\varepsilon m \log \log m}{2 \log m} + o \left(\frac{m \log \log m}{\log m} \right). \end{aligned} \quad (35)$$

Если слагаемое из правой части неравенства (21) отнесено к третьей группе, то также выполняются неравенства (25) и (32). Применяя оценки (26), (27), (28) и (33), с использованием (15) и (2) имеем

$$\begin{aligned}
& \log \left(\binom{u_1 + u_2 + u_3}{u_2 + u_3} \binom{u_2 + u_3}{u_2} \left(\frac{8 \log m}{\varepsilon \ln 2 \log \log m} \right)^{4u_2} \binom{(u_1 + u_2 + u_3)^2}{u_3} \right) \leq \\
& \leq (u_2 + u_3) \log \log m + 4u_2 \log \log m + u_3 \log m + u_3 \log \log m + o \left(\frac{m \log \log m}{\log m} \right) \leq \\
& \leq u_3 \log m + O \left(\frac{m \log \log m}{\log m} \right) \leq \\
& \leq \left(\frac{m}{\log m} - (2 + \varepsilon/2) \frac{m \log \log m}{(\log m)^2} - \left(1 - \frac{1}{2} \log 3 \right) u_2 \right) \log m + O \left(\frac{m \log \log m}{\log m} \right) < \\
& < m - \left(1 - \frac{1}{2} \log 3 \right) \frac{m}{\log \log \log m} + O \left(\frac{m \log \log m}{\log m} \right).
\end{aligned} \tag{36}$$

Таким образом, из (34), (35) и (36) следует, что двоичный логарифм любого слагаемого из (21) не превосходит величины

$$m - \frac{\varepsilon m \log \log m}{2 \log m} + o \left(\frac{m \log \log m}{\log m} \right).$$

Поэтому, учитывая, что в сумме из правой части неравенства (21) не более $8m^3$ слагаемых, получаем

$$\log R(m, \varepsilon) - m \leq -\frac{\varepsilon m \log \log m}{2 \log m} + o \left(\frac{m \log \log m}{\log m} \right),$$

а последнее выражение стремится к $-\infty$ при $m \rightarrow \infty$. Лемма 1 доказана.

Заключение

Помимо классических аддитивных цепочек, в различных криптографических приложениях, в первую очередь в алгоритмах, связанных с быстрыми вычислениями на эллиптических кривых, используется также аппарат цепочек из сложений и вычитаний [26, 27]. Утверждение теоремы 1 можно перенести и на такой класс вычислений.

Обозначим через $l^{as}(n)$ наименьшую длину цепочки из сложений и вычитаний для числа n (формальное определение цепочки из сложений и вычитаний отличается от определения аддитивной цепочки только тем, что произвольный шаг цепочки имеет вид либо $a_k = a_i + a_j$, либо $a_k = a_i - a_j$), а через $\hat{l}^{as}(n)$ — наименьшую длину цепочки для числа n , состоящей из шагов вида $a_k = a_i + a_j$, $a_k = a_i - a_j$ и $a_k = -a_i - a_j$. Положим

$$L^{as}(n) = \max_{k: k \leq n} l^{as}(k), \quad \hat{L}^{as}(n) = \max_{k: k \leq n} \hat{l}^{as}(k).$$

Теорема 2. Пусть $n \rightarrow \infty$. Тогда

$$L^{as}(n) \geq \hat{L}^{as}(n) \geq \log n + \frac{\log n}{\log \log n} \left(1 - (2 + o(1)) \frac{\log \log \log n}{\log \log n} \right).$$

Доказательство теоремы 2 несущественно сложнее доказательства теоремы 1. Технические особенности, связанные с наличием одной или двух дополнительных операций, можно проследить на примере доказательства нижней оценки из [28].

ЛИТЕРАТУРА

1. Кнут Д. Е. Искусство программирования. Т. 2. 3-е изд. М.: Издательский дом «Вильямс», 2000.
2. Scholz A. Jahresbericht // Deutsche Mathematiker-Vereinigung. 1937. В. 47. S. 41–42.
3. Subbarao M. V. Addition chains — some results and problems // Number Theory and Applications / ed. R. A. Mollin. NATO Advanced Science Institutes Series: Ser. C. Kluwer Academic Publisher Group, 1989. V. 265. P. 555–574.
4. Bos J. and Coster M. Addition chain heuristics // Crypto'89. LNCS. 1990. V. 435. P. 400–407.
5. Gordon D. M. A survey of fast exponentiation methods // J. Algorithms. 1998. V. 27. P. 129–146.
6. Thurber E. G. Efficient generation of minimal length addition chains // SIAM J. Comput. 1999. V. 28. P. 1247–1263.
7. Bernstein D. J. Pippenger's exponentiation algorithm. <http://cr.yp.to/papers/pippenger.pdf>, 2002.
8. Гашков С. Б. Задача об аддитивных цепочках и ее обобщения // Математическое просвещение. Третья серия. Вып. 15. М.: МЦНМО, 2011. С. 138–153.
9. Clift N. M. Calculating optimal addition chains // Computing. 2011. V. 91. P. 265–284.
10. Кочергин В. В. Уточнение оценок сложности вычисления одночленов и наборов степеней в задачах Беллмана и Кнута // Дискретный анализ и исследование операций. 2014. Т. 21. № 6. С. 51–72.
11. Järvinen K, Dimitrov V., and Azarderakhsh R. A generalization of addition chains and fast inversions in binary fields // IEEE Trans. Computers. 2015. V. 64(9). P. 2421–2432.
12. Von zur Gathen J. and Nöcker M. Exponentiation in finite fields: theory and practice // LNCS. 1997. V. 1255. P. 88–113.
13. Смарт Н. Криптография. М.: Техносфера, 2005.
14. Гашков С. Б., Сергеев И. С. О применении метода аддитивных цепочек к инвертированию в конечных полях // Дискретная математика. 2006. Т. 18. № 4. С. 56–72.
15. Brauer A. On addition chains // Bull. Amer. Math. Soc. 1939. V. 45. P. 736–739.
16. Erdos P. Remarks on number theory, III: On addition chains // Acta Arith. 1960. V. 6. P. 77–81.
17. Ильин А. М. Об аддитивных цепочках чисел // Проблемы кибернетики. Вып. 13. М.: Физматлит, 1965. С. 245–248.
18. Schönhage A. A. Lower bound for the length of addition chains // Theor. Comput. Sci. 1975. V. 1. P. 1–12.
19. Сэвидж Д. Е. Сложность вычислений. М.: Факториал, 1998.
20. Нигматуллин Р. Г. Сложность булевых функций. М.: Наука, 1991.
21. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.
22. Riordan J. and Shannon C. E. The number of two-terminal series-parallel networks // J. Math. Phys. Mass. Inst. Tech. 1942. V. 21. No. 2. P. 83–93. Рус. пер.: Риордан Дж., Шеннон К. Число двухполюсных параллельно-последовательных сетей / сб. Шеннон К. Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 46–58.
23. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. М.: Наука, 1996. С. 189–214.
24. Ложкин С. А. Асимптотические оценки высокой степени точности для сложности реализации булевских функций схемами из функциональных элементов // Труды II Меж-

- дунар. конф. «Дискретные модели в теории управляющих систем» (23–28 июня 1997 г.). М.: Диалог-МГУ, 1997. С. 37–39.
25. *Кочергин В. В., Кочергин Д. В.* Уточнение асимптотического поведения сложности сборки слов схемами конкатенации // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. 2016. № 2. С. 12–18.
 26. *Volger H.* Some results on addition/subtraction chains // Inform. Proc. Lett. 1985. V. 20. P. 155–160.
 27. *Morain F. and Olivos J.* Speeding up the computation on an elliptic curve using addition-subtraction chains // Informatique Théorique et Applications. 1990. V. 24. P. 531–544.
 28. *Кочергин В. В.* О сложности вычислений одночленов и наборов степеней // Дискретный анализ. Новосибирск: Изд-во Института математики СО РАН, 1994. С. 94–107.

REFERENCES

1. *Knuth D. E.* The art of computer programming, vol. 2, third edition. Reading, Massachusetts, Addison-Wesley, 1997.
2. *Scholz A.* Jahresbericht. Deutsche Mathematiker-Vereinigung, 1937, B. 47, S. 41–42.
3. *Subbarao M. V.* Addition chains — some results and problems. Number Theory and Applications. Ed. R. A. Mollin. NATO Advanced Science Institutes Series, Ser. C. Kluwer Academic Publisher Group, 1989, vol. 265, pp. 555–574.
4. *Bos J. and Coster M.* Addition chain heuristics. Crypto'89, LNCS, 1990, vol. 435, pp. 400–407.
5. *Gordon D. M.* A survey of fast exponentiation methods. J. Algorithms, 1998, vol. 27, pp. 129–146.
6. *Thurber E. G.* Efficient generation of minimal length addition chains. SIAM J. Comput., 1999, vol. 28, pp. 1247–1263.
7. *Bernstein D. J.* Pippenger's exponentiation algorithm. <http://cr.yp.to/papers/pippenger.pdf>, 2002.
8. *Gashkov S. B.* Zadacha ob additivnykh tsepochkakh i eye obobshcheniya [Addition chains problem and its generalizations]. Matematicheskoye Prosveshcheniye. Third series, vol. 15. Moscow, MTsNMO, 2011, pp. 138–153. (in Russian)
9. *Clift N. M.* Calculating optimal addition chains. Computing, 2011, vol. 91, pp. 265–284.
10. *Kochergin V. V.* Improvement of the estimates of the computational complexity for monomials and sets of powers in Bellman's and Knuth's problems. J. Appl. Industr. Math., 2015, vol. 9, no. 1, pp. 68–82.
11. *Järvinen K, Dimitrov V., and Azarderakhsh R.* A generalization of addition chains and fast inversions in binary fields. IEEE Trans. Computers, 2015, vol. 64(9), pp. 2421–2432.
12. *Von zur Gathen J. and Nöcker M.* Exponentiation in finite fields: theory and practice. LNCS, 1997, vol. 1255, pp. 88–113.
13. *Smart N.* Cryptography: An Introduction (3rd edition). McGraw — Hill, 2003.
14. *Gashkov S. B. and Sergeev I. S.* An application of the method of additive chains to inversion in finite fields. Discr. Math. Appl., 2006, vol. 16, no. 6, pp. 601–618.
15. *Brauer A.* On addition chains. Bull. Amer. Math. Soc., 1939, vol. 45, pp. 736–739.
16. *Erdos P.* Remarks on number theory, III: On addition chains. Acta Arith., 1960, vol. 6, pp. 77–81.
17. *И'ин А. М.* Ob additivnykh tsepochkakh chisel [On addition chains of numbers]. Problemy Kibernetiki, vol. 13. Moscow, Fizmatlit Publ., 1965, pp. 245–248. (in Russian)
18. *Schönhage A. A.* Lower bound for the lenght of addition chains. Theor. Comput. Sci., 1975, vol. 1, pp. 1–12.
19. *Savage J. E.* The Complexity of Computing. New York, Wiley, 1976.

20. *Nigmatullin R. G.* Slozhnost' bulevykh funktsiy [The Complexity of Boolean Functions]. Moscow, Nauka Publ., 1991. (in Russian)
21. *Lupanov O. B.* Asimptoticheskie otsenki slozhnosti upravlyayushchikh sistem [Asymptotic Estimations of Complexity of Control Systems]. Moscow, MSU Publ., 1984. (in Russian)
22. *Riordan J. and Shannon C. E.* The number of two-terminal series-parallel networks. J. Math. Phys. Mass. Inst. Tech., 1942, vol. 21, no. 2, pp. 83–93.
23. *Lozhkin S. A.* Otsenki vysokoy stepeni tochnosti dlya slozhnosti upravlyayushchikh sistem iz nekotorykh klassov [More accurate estimations of complexity of control systems for some classes]. Matematicheskiye Voprosy Kibernetiki, vol. 6, Moscow, Nauka Publ., 1996, pp. 189–214. (in Russian)
24. *Lozhkin S. A.* Asimptoticheskiye otsenki vysokoy stepeni tochnosti dlya slozhnosti realizatsii bulevskikh funktsiy skhemami iz funktsional'nykh elementov [More accurate asymptotic estimations of complexity of Boolean functions realization by logic circuits]. Proc. II Intern. conf. "Diskretnye modeli v teorii upravlyayushchikh sistem" (22–23 June 1997), Moscow, Dialog-MSU Publ., 1997, pp. 37–39. (in Russian)
25. *Kochergin V. V. and Kochergin D. V.* Revision of asymptotic behavior of the complexity of word assembly by concatenation circuits. Moscow University Math. Bull., 2016, vol. 71, iss. 2, pp. 55–60.
26. *Volger H.* Some results on addition/subtraction chains. Inform. Proc. Lett., 1985, vol. 20, pp. 155–160.
27. *Morain F. and Olivos J.* Speeding up the computation on an elliptic curve using addition-subtraction chains. Informatique Théorique et Applications, 1990, vol. 24, pp. 531–544.
28. *Kochergin V. V.* On the complexity of computations of monomials and tuples of powers. Siberian Adv. Math., 1996, vol. 6, no. 1, pp. 71–86.